1. **Name of Course/Module**: Cryptography and Data Security  
2. **Course Code**: TCD2221  
3. **Status of Subject**: Major for B.IT Data Communications And Networking  
4. **MQF Level/Stage**: Bachelor Degree – MQF Level 6  
5. **Version** (state the date of the last Senate approval): June 2012  
6. **Requirement for Registration**: TCS 1011 Data Structures and Algorithms  
7. **Name(s) of academic/teaching staff**: K.Jayakkumar, Sia Sie Tung, Asrul Hadi b Yaacob  
8. **Semester and Year offered**: Trimester 2 (Gamma Level)  
9. **Objective of the course/module in the programme**:  
   
   To introduce to the students the science and study of methods of data protection computer and communication systems from unauthorized disclosure and modification, to show how to develop techniques for verification, identification, key safeguarding schemes and key distribution protocols and to introduce students to different methods of encrypting data for security purposes.  
10. **Learning Outcomes**:  
   
   At the completion of the subject, students should be able to:  
   
   **LO1**: Recall the definitions of all the concepts and technical terms related to cryptography and data security. (Cognitive, Level 1)  
   
   **LO2**: Adopt and make use of the concepts of message authentication and hash functions in cryptographic applications such as digital signature. (Cognitive, Level 5)  
   
   **LO3**: Explain and differentiate between the various cryptographic schemes such as symmetric encryption, asymmetric encryption, authentication, key distribution and key management. (Cognitive, Level 6)  
   
   **LO4**: Analyse the security of some simple cryptographic schemes. (Affective, Level 5)  
   
   **LO5**: Implement some simple cryptographic schemes. (Cognitive, Level 4)  
11. **Synopsis**:  
   
   This course covers symmetric and asymmetric encryption methods, cryptographic techniques, security and legality issues in cryptography and data security.  
   
   Kursus ini meliputi, kaedah-kaedah penyuntingan, teknik-teknik kriptografi, isu-isu keselamatan dan kesahihan dalam kriptografi dan keselamatan data.  
12. **Mapping of Subject to Programme Outcomes**:  

<table>
<thead>
<tr>
<th>Programme Outcomes</th>
<th>% of Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1: Apply soft skills in work and career related activities</td>
<td>25.00</td>
</tr>
</tbody>
</table>
PO7: Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to data communications and networking 37.50

PO8: Apply principles and knowledge of data communications and networking in relevant areas 37.50

13. Assessment Methods and Types :

<table>
<thead>
<tr>
<th>Method and Type</th>
<th>Description/Details</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>Written Test</td>
<td>30%</td>
</tr>
<tr>
<td>Quiz</td>
<td>Written Quiz</td>
<td>5%</td>
</tr>
<tr>
<td>Assignment</td>
<td>Report &amp; Presentation</td>
<td>15%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>Written Exam</td>
<td>50%</td>
</tr>
</tbody>
</table>

14. Details of Subject

<table>
<thead>
<tr>
<th>Topics</th>
<th>Mode of Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture</td>
<td>Tutorial</td>
</tr>
<tr>
<td>1. Introduction</td>
<td></td>
</tr>
<tr>
<td>2. Symmetric Encryption</td>
<td></td>
</tr>
<tr>
<td>3. Number Theory</td>
<td></td>
</tr>
<tr>
<td>4. Asymmetric Encryption</td>
<td></td>
</tr>
</tbody>
</table>

1. Introduction
- Definition of the Cryptographic System: Encryption & Decryption, Symmetric & Asymmetric Ciphers
- Background History of Cryptography
- Steganography
- Message Security Threats: Passive & Active attacks
- Types of Cryptanalytic Attacks (ciphertext only, known plaintext, chosen plaintext, chosen ciphertext, chosen text)
- The goals of cryptography and data security: Confidentiality, Integrity, Authenticity.

2. Symmetric Encryption
- Brief Introduction to Symmetric Key Encryption Model
- Classical ciphers: Transposition ciphers, Substitution ciphers, Knapsack ciphers
- Product Cipher: DES and triple DES, brief introduction to AES
- Symmetric Block Cipher Characteristics: Block Cipher Modes of Operations (ECB, CBC, CFB, CTR, OFB).
- Stream Cipher and One-Time Pads (Perfect Secrecy).

3. Number Theory
- Modular Arithmetic
- Prime Numbers
- Greatest Common Divisor (GCD)
- Multiplicative Inverse
- Fermat’s Little Theorem
- Euler Totient Function
- Euler’s Theorem

4. Asymmetric Encryption
- Brief Introduction to the Asymmetric Key Encryption Model
- Asymmetric (Public-Key) Encryption Characteristics
- Public Key Encryption: RSA
### 5. Authentication
- Password Authentication,
- Message Authentication Code (MAC) properties and basic uses of MAC
- Hash properties and basic uses of hash
- Brief Introduction to the Digital Signature Model and Threats to Digital Signatures (i.e. Replay Attacks)

### 6. Key Distribution, Key Management & Digital Certificates
- Brief introduction to Key Distribution Methods
- Simple Key Distribution (Merkle)
- Key Management
- Diffie-Hellman Key Exchange
- Public Key Infrastructure (PKI): Public Key Certificates, Certificate Authority (CA) & Certificate Servers

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>

### 15. Tutorials
- Descriptions of different cryptographic systems
- Implementation of different types of ciphers
- Calculation using different theorem in number theory
- Implementation of asymmetric encryption
- Implementation of key distribution, key management & digital certificates

### 16. Total Student Learning Time (SLT) Face to Face Total Guided and Independent Learning

<table>
<thead>
<tr>
<th></th>
<th>Face to Face (Hour)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>Tutorials</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Laboratory/Practical Presentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignment</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>Mid Term Test</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Final Exam</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>Quizzes</td>
<td>2 times</td>
<td>2</td>
</tr>
<tr>
<td>Sub Total</td>
<td>45</td>
<td>79</td>
</tr>
<tr>
<td>Total SLT</td>
<td>124/40 = 3.1 =&gt; 3</td>
<td></td>
</tr>
</tbody>
</table>

### 17. Credit Value
- 3

### 18. Reading Materials:

- **Textbook**

- **Reference Materials**
Appendix (to be compiled when submitting the complete syllabus for the programme):

1. Mission and Vision of the University and Faculty
2. Mapping of Programme Objectives to Vision and Mission of Faculty and University
3. Mapping of Programme Outcome to Programme Objectives
4. Programme Objective and Outcomes (Measurement and Descriptions)